(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : 0 621 570 A1

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : 94400814.3

(51) Int. Cl.[5] : G07F 7/12

(22) Date de dépôt : 14.04.94

(30) Priorité : 16.04.93 FR 9304515

(43) Date de publication de la demande :
26.10.94 Bulletin 94/43

(84) Etats contractants désignés :
DE FR GB

(71) Demandeur : FRANCE TELECOM
Etablissement autonome de droit public,
6, Place d'Alleray
F-75015 Paris (FR)

(71) Demandeur : LA POSTE
4, Quai du Point du Jour
F-92777 Boulogne Billancourt Cédex (FR)

(72) Inventeur : Pailles, Jean-Claude
4, rue des Loisirs
F-14610 Epron (FR)
Inventeur : Depret, Eric
52, rue Galliéni
F-14000 Caen (FR)
Inventeur : Hiolle, Philippe
1201 Quartier Grande Delle
F-14200 Herouville Saint Clair (FR)

(74) Mandataire : Signore, Robert
c/o SOCIETE DE PROTECTION DES INVENTIONS
25, rue de Ponthieu
F-75008 Paris (FR)

(54) Procédé de mise à jour d'une carte à mémoire.

(57) La carte contient notamment, un compteur irréversible, un solde et un certificat prouvant l'intégrité des informations précédentes. Le contenu de la carte ne peut être mis à jour que par des terminaux connaissant les secrets de calcul du certificat. Grâce au compteur irréversible qui intervient dans le calcul du certificat, il n'est pas possible de recharger dans la carte un contenu antérieur (solde/certificat), car un tel rechargement nécessite d'incrémenter le compteur, ce qui rend caduc le certificat antérieur.

EP 0 621 570 A1

Domaine technique

La présente invention a pour objet un procédé de mise à jour d'une carte à mémoire. Elle trouve une application dans ce qu'on appelle la monnaie électronique et plus particulièrement dans les systèmes à prépaiement dits ouverts. On désigne par là des systèmes impliquant un organisme émetteur de monnaie électronique, des utilisateurs possédant des cartes préchargées par l'émetteur, et des terminaux aptes à fournir certaines prestations, à débiter les cartes en conséquence et à collecter les montants provenant de plusieurs cartes. L'organisme propriétaire de ces terminaux est rétribué par l'émetteur selon la quantité d'unités qu'il a collectées. Le caractère "ouvert" de certains de ces systèmes vient de ce que l'organisme émetteur n'est pas nécessairement confondu avec les prestataires possédant les terminaux.

Si l'invention s'applique de manière privilégiée à de tels systèmes, parce qu'elle permet de résoudre certains problèmes liés au caractère "ouvert", elle n'est pas limitée pour autant à ces seuls systèmes et pourrait aussi bien s'appliquer à des systèmes fermés, où l'organisme émetteur serait le propriétaire des terminaux.

Etat de la technique antérieure

Comme tous les systèmes à cartes portatives, les systèmes à prépaiement posent des problèmes de sécurité. Le problème est d'autant plus ardu pour les systèmes ouverts que les terminaux doivent prouver à l'organisme émetteur l'authenticité des montants qu'ils ont collectés. A cette fin, chaque terminal doit être équipé d'un module de sécurité.

Ces problèmes de sécurité peuvent être mieux perçus en passant en revue quelques risques de fraudes qu'il faut éviter :

risque a) : altération des données échangées :

il ne doit pas être possible, par interposition de dispositifs informatiques entre une carte et un module de sécurité, de modifier les données transmises pour, par exemple, créditer un module de sécurité de plus d'unités qu'il n'en a été débité dans la carte ;

risque b) : réutilisation des données échangées :

il ne doit pas être possible de répéter les échanges de données, par exemple pour créditer plusieurs fois un même module de sécurité à partir d'un seul débit d'une carte ;

risque c) : interposition d'un autre module de sécurité :

il ne doit pas être possible d'interposer un second module de sécurité et de créditer les deux modules de sécurité à partir d'un seul débit d'une carte ;

risque d) : altération du contenu d'une carte :

il ne doit pas être possible d'altérer le contenu d'une carte de façon à en augmenter illicitement le pouvoir d'achat.

Tous ces problèmes peuvent être résolus par l'introduction, dans la carte, d'un microprocesseur aptes à effectuer diverses opérations de vérification, embrouillage des données, authentification, signature, etc...

Cette solution donne satisfaction à certains égards. Elle présente néanmoins l'inconvénient d'être coûteuse car elle nécessite l'introduction d'un microprocesseur dans chaque carte.

On connaît par le document EP-A-0 423 035, un système de paiement ou de transfert d'informations par carte à mémoire électronique porte-monnaie, qui évite l'emploi d'un microprocesseur. Ce système comprend diverses zones mémoire, dont une zone contenant l'identité du titulaire, une zone contenant un certificat, une zone contenant un compteur, une zone contenant un solde et une zone contenant un code secret.

Le compteur compte le nombre d'opérations financières effectuées avec la carte. Le certificat est fonction de l'identité du titulaire, du contenu du compteur et du solde.

Ce système ne résout pas parfaitement les problèmes de sécurité, en ce sens qu'il n'évite pas que de la fausse monnaie puisse être créée. En effet, les zones mémoire contenant le certificat et le solde sont effaçables et inscriptibles sans aucune contrainte. Rien n'empêche donc de débiter une carte porte-monnaie de 10 unités par exemple et de créditer deux terminaux de 10 unités. On aura ainsi créé 10 unités de fausse monnaie.

La présente invention a justement pour but de remédier à cet inconvénient.

Exposé de l'invention

La présente invention reprend certaines des opérations divulguées par le document cité (incrémentation d'un compteur, formation d'un certificat), mais elle ajoute à celles-ci des opérations qui évitent tout risque de création de fausse monnaie. Pour cela, le calcul du certificat tient compte de l'identité du module de sécurité, de sorte que deux certificats calculés par deux terminaux différents pour une même carte porte-monnaie et pour la même transaction seront nécessairement différents. Par ailleurs, pour effacer le certificat et le réécrire,

il faudra nécessairement incrémenter le compteur. Enfin, les terminaux authentifient la carte porte-monnaie et son contenu avant et après la transaction.

De façon précise, la présente invention a donc pour objet un procédé de mise à jour d'une information (tr) contenue dans une partie (Tr) d'une mémoire (M) contenue dans une carte à mémoire (CM), à l'aide d'un terminal (T) équipé d'un module de sécurité (MS), la mémoire (M) contenant une zone compteur (C), le contenu de la partie (Tr) de la mémoire (M) à mettre à jour comprenant un certifcat (d) contenu dans une zone (D) de la partie (Tr), ce certificat étant une fonction déterminée (g) de l'identité (i) de la carte, d'un solde (b) contenu dans une autre zone (B), du contenu (c) de la zone compteur (C), ce procédé consistant à :

- incrémenter d'une unité le contenu (c) de la zone compteur (C) avant toute mise à jour de la partie (Tr),
- effacer l'ancien contenu (tr) de la partie (Tr) de la mémoire (M) et y inscrire à la place un nouveau contenu (tr') mis à jour,

ce procédé étant caractérisé par le fait que :

- le certificat (d) est en outre une fonction de l'identité (j) du module de sécurité (MS) ayant effectué la dernière mise à jour,
- pour effacer le certificat contenu dans la zone (D) et réécrire le certificat mis à jour, on incrémente la zone compteur (C),
- le terminal (T) authentifie la carte (CM) et son contenu (m) avant et après la mise à jour.

Les cartes peuvent être authentifiées grâce à un processus challenge-réponse qui est classique en sécurité informatique : le terminal envoie à la carte un challenge x, qui est choisi en général aléatoirement ou différent des valeurs déjà utilisées. La carte calcule une fonction Y=f(x,m) où m représente le contenu de sa mémoire. Le terminal peut alors acquérir la certitude que la carte est authentique, ainsi que son contenu, en faisant de son côté le même calcul pour vérifier Y. Pour que ce processus ne soit pas imitable, il faut qu'il y ait un secret quelque part : par exemple, la mémoire doit contenir une clé, non lisible de l'extérieur, mais que le terminal ou l'ordinateur qui lui est raccordé connaît ou sait reconstituer.Ainsi, le terminal peut authentifier la carte et son contenu.

De préférence, le solde (b) contenu dans la zone (B) est un solde financier, le procédé étant alors un procédé de paiement correspondant à une prestation.

Pour prévenir toute possibilité de retour en arrière (changer b',d' en b,d, (ce qui aurait pour effet d'effacer la dernière consommation), un mécanisme de "cliquet" est mis en oeuvre grâce à la zone mémoire C. La carte comprend des moyens tels que le contenu de la zone C doit être incrémenté avant la mise à jour des zones B, D et J, (ce qui nécessite un effacement préalable de ces zones). La zone C est une zone qui, au départ, peut être à zéro, et dans laquelle des bits peuvent être simplement écrits, mais non effacés.

Le calcul du certificat d prend en compte la valeur c de ce compteur. Ainsi, modifier (b',d') en (b,d) n'est pas possible sans que soit incrémenté c. Mais alors le certificat d n'est plus correct, puisque calculé avec le c précédent.

Le calcul du certificat d doit aussi prendre en compte le numéro j du module de sécurité, de façon à lier, lors d'une transaction, une carte à un module de sécurité particulier et éviter la fraude de type c, telle que décrite plus haut.

Lorsque le procédé de l'invention est un procédé de paiement, il comporte, de préférence, les opérations suivantes :

a) vérifier qu'un certificat (d) contenu dans une zone (D) de la partie (Tr) de la carte est bien une fonction déterminée (g) de l'identité de la carte (i), de son solde (b), du contenu (c) d'une zone mémoire (C) jouant le rôle de compteur, et de l'identité (j) du dernier module de sécurité ayant effectué la dernière transaction,

b) calculer, dans le module de sécurité (MS), un nouveau solde (b') qui diffère de l'ancien (b) d'un certain nombre d'unités (n), correspondant à une prestation,

c) calculer, dans le module de sécurité (MS), un contenu de compteur (c') égal à l'ancien contenu (c) augmenté d'une unité (c'=c+1),

d) calculer un nouveau certificat (d') égal à ladite fonction (g) de l'identité de la carte (i), du nouveau solde (b'), du nouveau contenu (c') du compteur et de l'identité (j') du module de sécurité (MS),

e) incrémenter d'une unité le contenu (c) de la zone mémoire (C) de la carte jouant le rôle de compteur (c'=c+1),

f) si et seulement si ce contenu (c') a été effectivement incrémenté, il est possible d'effacer de la partie (Tr) son ancien contenu (tr) constitué par l'ancien solde (b), l'ancien certificat (d) et l'ancienne identité (j) du dernier module de sécurité utilisé et y inscrire à la place un nouveau contenu (tr') constitué par le nouveau solde (b'), le nouveau certificat (d') et l'identité (j') du module de sécurité du terminal,

g) authentifier par le module de sécurité (MS) la carte (CM) et au moins l'identité (j) du nouveau contenu (tr') de la zone (Tr),

h) en cas d'authenticité, modifier le solde (s) du module de sécurité de la quantité (n) correspondant à la

modification du solde de la carte (s'=s+n).

Ce procédé permet bien d'éviter les risques définis plus haut, à savoir, respectivement :

risque a) le module de sécurité authentifie la carte au début de la transaction et après mise à jour des données écrites dans la carte ; il n'est donc pas possible de modifier les données transmises ;

risque b) le module de sécurité authentifie la carte avant et après la transaction et choisit les challenges ; on ne peut donc lui soumettre à nouveau les données d'un premier échange telles quelles ;

risque c) si la transaction devait s'effectuer entre deux modules de sécurité différents, donc d'identités différentes respectivement, j1 et j2, il faudrait, pour une même valeur c de la zone compteur C, inscrire deux séries de données différentes, l'une T1 relative à j1 et l'autre, T2, relative à j2 ; mais pour effacer T1 afin d'écrire T2, il faudrait nécessairement incrémenter le contenu de la zone compteur C, ce qui rendrait invalide T2 ; on ne peut donc créditer deux modules de sécurité à partir d'un même débit affectant une seule carte.

risque d) on ne peut modifier le solde b car le certificat d dépendant de façon secrète du solde b, il est impossible de trouver la valeur correspondante de d, et une valeur fausse serait détectée lors de la transaction suivante ; pour remettre la carte dans un état antérieur, il faudrait donc effacer son contenu c, ce qui impliquerait d'incrémenter le contenu du compteur C ; les anciennes valeurs du certificat d serait alors incorrectes, le module de sécurité impliqué dans la transaction le détecterait et la carte ne serait donc plus utilisable.

Exposé détaillé d'un mode de réalisation

On va décrire, ci-après, une procédure détaillée d'échange d'ordres et de données entre une carte à mémoire, un terminal et son module de sécurité. Les lettres majuscules désignent des zones mémoire où des dispositifs alors que les minuscules correspondantes désignent le contenu de ces zones. La carte à mémoire est notée CM, son identité est i. Le terminal est noté T. Le module de sécurité en service est noté MS et son identité est notée j', sachant que celle du module ayant effectué la transaction précédente était j.

Les opérations mises en oeuvre sont alors les suivantes :

1. T demande à MS de choisir un aléa ;
2. MS choisit et mémorise un aléa, soit x ;
3. MS transmet x à T ;
4. T demande à CM de lire le contenu m de la mémoire M ;
5. CM lit M et transmet m à T ;
6. T demande à CM de s'authentifier à l'aide de l'aléa x ;
7. CM calcule Y=f(m,x) ;
8 CM transmet Y a T ;
9. T transmet Y et m à MS ;
10. MS calcule f(x,m) et vérifie que Y est bien égal à f(x,m)
11. T demande à MS de vérifier le certificat d ;
12. MS calcule D=g(i,b,c,j) ;
13. T communique à MS le débit à effectuer n ;
14. MS calcule la nouvelle valeur du solde d'=d-n, incrémente c par c'=c+1 et calcule d'=g(i,b',c',j') ;
15. MS transmet à T les mises à jour d', j', b' ;
16. T demande à CM d'écrire un 1 dans la zone C, d'effacer le contenu tr de la zone de travail Tr, d'y écrire le nouveau contenu tr' formé par j', b', d' ;
17. T demande à MS de choisir un nouvel aléa ;
18. MS choisit et mémorise un aléa x' ;
19. MS adresse x' à T ;
20. T demande à CM de s'authentifier avec son nouveau contenu m' ;
21. CM calcule Y'=f(x',m') ;
22. CM transmet à T la valeur de Y' ;
23. T demande à MS de vérifier l'authenticité de Y' ;
24. MS vérifie que m' correspond bien à i', c', j', b', d' et vérifie que Y'=f(x',m') ;
25. si la vérification est positive, MS augmente son solde de n.

Les opérations qui précèdent aboutissent à la diminution du solde de la carte et à l'augmentation du montant collecté par le terminal. Il va de soi qu'on peut appliquer la même suite d'opérations pour recharger une carte et augmenter son solde, et diminuer d'autant un terminal de rechargement.

Dans les exemples qui précèdent, (m) représente le contenu des données dans la carte (CM) . Mais il est possible de ne pas incorporer dans (m) les données du certificat (d) et celles du solde (b). En effet, ces données

sont authentifiables indirectement par le fait que Y est une fonction notamment de (j). Ceci peut simplifier la réalisation.

Revendications

1. Procédé de mise à jour d'une information (tr) contenue dans une partie (Tr) d'une mémoire (M) contenue dans une carte à mémoire (CM), à l'aide d'un terminal (T) équipé d'un module de sécurité (MS), la mémoire (M) contenant une zone compteur (C), le contenu de la partie (Tr) de la mémoire (M) à mettre à jour comprenant un certificat (d) contenu dans une zone (D) de la partie (Tr), ce certificat étant une fonction déterminée (g) de l'identité (i) de la carte, d'un solde (b) contenu dans une autre zone (B), du contenu (c) de la zone compteur (C), ce procédé consistant à :
   - incrémenter d'une unité le contenu (c) de la zone compteur (C) avant toute mise à jour de la partie (Tr),
   - effacer l'ancien contenu (tr) de la partie (Tr) de la mémoire (M) et y inscrire à la place un nouveau contenu (tr') mis à jour,

   ce procédé étant caractérisé par le fait que :
   - le certificat (d) est en outre une fonction de l'identité (j) du module de sécurité (MS) ayant effectué la dernière mise à jour,
   - pour effacer le certificat contenu dans la zone (D) et réécrire le certificat mis à jour, on incrémente la zone compteur (C),
   - le terminal (T) authentifie la carte (CM) et son contenu (m) avant et après la mise à jour.

2. Procédé selon la revendication 1, caractérisé par le fait que le solde (b) contenu dans la zone (B) est un solde financier, le procédé étant alors un procédé de paiement correspondant à une prestation.

3. Procédé selon la revendication 2, caractérisé par le fait qu'il consiste à :
   a) vérifier qu'un certificat (d) contenu dans une zone (D) de la partie (Tr) est bien une fonction déterminée (g) de l'identité de la carte (i), de son solde (b), du contenu (c) d'une zone mémoire (C) jouant le rôle de compteur, et de l'identité (j) du dernier module de sécurité ayant effectué la dernière transaction,
   b) calculer, dans le module de sécurité (MS), un nouveau solde (b') qui diffère de l'ancien (b) d'un certain nombre d'unités (n) correspondant à une prestation,
   c) calculer, dans le module de sécurité (MS), un contenu de compteur (c') égal à l'ancien contenu (c) augmenté d'une unité (c'=c+1),
   d) calculer un nouveau certificat (d') égal à ladite fonction (g) de l'identité de la carte (i), du nouveau solde (b'), du nouveau contenu (c') du compteur et de l'identité (j') du module de sécurité (MS),
   e) incrémenter d'une unité le contenu (c) de la zone mémoire (C) de la carte jouant le rôle de compteur (c'=c+1),
   f) si et seulement si ce contenu (c') a été effectivement incrémenté, effacer de la partie (Tr) son ancien contenu (tr) constitué par l'ancien solde (b), l'ancien certificat (d) et l'ancienne identité (j) du dernier module de sécurité utilisé et y inscrire à la place un nouveau contenu (tr') constitué par le nouveau solde (b'), le nouveau certificat (d') et l'identité (j') du module de sécurité du terminal,
   g) authentifier par le module de sécurité (MS) la carte (CM) et au moins l'identité (j) du nouveau contenu (tr') de la partie (Tr),
   h) en cas d'authenticité, modifier le solde (s) du module de sécurité de la quantité (n) correspondant à la modification du solde de la carte (s'=s+n).

4. Procédé selon la revendication 3, caractérisé par le fait que, pour authentifier une carte (CM) lors de son introduction dans un terminal (T) :
   - le module de sécurité (MS) choisit et mémorise un aléa (x) et l'adresse au terminal (T),
   - le terminal (T) adresse cet aléa (x) à la carte (CM),
   - la carte (CM) lit le contenu de sa mémoire (m) et l'adresse au terminal (T),
   - le module de sécurité (MS) calcule une fonction Y=f(x,m) de l'aléa (x) et du contenu (m) de la mémoire (M),
   - la carte calcule une fonction Y=f(m,x) de son contenu (m) et de l'aléa (x) reçu et adresse cette fonction (Y) au terminal,
   - le module de sécurité (MS) teste que le résultat de la fonction (Y) reçue de la carte est bien identique au résultat de la fonction qu'il a calculée.

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 94 40 0814

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.5)
D,Y	EP-A-0 423 035 (GEMPLUS CARD INTERNATIONAL) * abrégé; revendications; figures * * colonne 3, ligne 47 - colonne 6, ligne 14 *	1-3	G07F7/12
Y	EP-A-0 152 703 (FAIRVIEW PARTNERS) * abrégé; figures 3,4 * * page 9, ligne 32 - page 11, ligne 16 *	1-3	
A	EP-A-0 096 599 (CII HONEYWELL BULL) * abrégé; revendications; figure *	1,4	
A	FR-A-2 246 913 (GRETAG) * page 6, ligne 36 - page 9, ligne 6 *	1-3	
			DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)
			G07F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	2 Août 1994	David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P01C02)